Banking and Bookkeeping

Bit of history

Double-entry bookkeeping

- Extremely important innovation
- Developed in late medieval times
  - Banks grew bigger
  - Developed branches
  - Owning families started hiring outside managers
- Double-entry bookkeeping was invented to reduce risk of fraud

Double-entry bookkeeping (2)

- Each transaction is recorded in two separate books
  - Credit in one, debit in another
- Example: customer buys goods
  - Credit „goods in warehouse”, debit „unpaid bills”
- Example: customer pays for goods
  - Credit „unpaid bills”, debit „cash”

Double-entry bookkeeping (3)

- Important invariant: books must balance
  - This means: all books must add up to zero
  - Assets and liabilities must be equal
- The books are kept by different clerks
- Books are balanced at the end of month
- Books in branches can be balanced separately
- At the end of the year, records are audited by external parties

E-commerce

- With the invention of telegraph, people started using it for business
  - Sending stock market information
  - Sending bills, purchase orders, money transfers
- Problems were the same as today
  - How to ensure that data is not modified in transit?
  - Who am I talking to?
  - Will I get my money? Will I get my goods?

Computerizing bookkeeping

- Accounting systems generally implement double-entry bookkeeping
- ... or do they?
  - Database is just list of transactions?
  - Each book is just a database table/file?
  - Systems administrator has access to all the files?

Typical bank IS

- Account master file
  - Customer's current balance
  - Customer's transaction history
- Ledgers – keep track of assets
- Journals – pending transactions that are not entered into system
- Audit trail – log of actions by personnel

Security measures

- Books are balanced each night
- Different teams work on different subsystems
- Regular code audits
- Testing by separate test team
- Separate production and development environments

Clark-Wilson security policy model

- UDI – unconstrained data item
- CDI – constrained data item
- IVP – identity verification procedure
- TP – transformation procedure
- Access control by triplets: (subject, TP, CDI)

Clark-Wilson rules

- For every CDI, there must be IVP for validating it
- The application of TP to CDI must maintain its integrity
- Only TP can change CDI
- Subjects can initiate certain TPs on certain CDIs
- Triples must enforce separation of duty policy
- Certain TPs on UDIs can produce CDIs

Clark-Wilson rules (2)

- Each application of TP must write to append-only CDI
  - There must be enough information to reconstruct the action
- Subjects must be authenticated to invoke a TP
- Only special subjects can modify authorization-related lists

About Clark-Wilson model

- Main focus is maintaining consistent state
- Because of dual control, the system must be able to store partial transactions
- It does not deal with correctness
- It does not deal with people problems

Protecting against insiders

- This is main topic in banking and accounting
- Obvious means: laws, rules, auditing
- Technical means: use **separation of duty**
  - Dual control
  - Functional separation

Dual control

- Also called: split responsibility
- Several people must act together to authorize transaction
- Example: door that must be opened by two persons
- Example: require two signatures on some order

Functional separation

- Different people act on transaction on different times
- Example: purchasing
  - Manager forwards purchasing decision to purchasing department
  - PD clerk creates purchase order
  - Warehouse clerk records arrival of goods
  - Accounting receives invoice and compares it with purchase order and arrival info
  - Accounting manager signs the check

Functional separation (2)

- And more:
  - Department's costs increase
  - Bosses review profit reports
  - Internal audit can investigate department
  - External audit can investigate department
  - Company lawyers will make effort to recover money

What to consider

- Cultural issues
  - Are managers' signatures common?
- Environment
  - Is it a bank or accounting department of a small company
- Human factors
  - Authoritarian managers, motivation of staff
- Single points of failure
  - e.g. sysadmin creates two accounts

What to consider (2)

- In general, system administrators must be trusted
  - Separate production and development systems
  - Separate development and maintenance crew
- Other top people are trusted too
  - Find out who they are and try to minimize their numbers (and pay them well)
- Dual control does not work between organizations

Some statistics

- According to Ernst and Young study...
- 85% of frauds were done by own employees
- Half of them were from management
- Big frauds usually involve lax internal controls

Some example cases

- Password reset clerk changed company's Internet bank password
- Bank had special account for pending, problematic transactions, employee withdrew money from that account
- Clerk in education authority created a fictious school
- Bank clerk changed customer's address, changed to his, issued ATM card and PIN

Some lessons

- It is not always obvious which transactions are security sensitive
- Environment changes can affect security of the system
- Use customer complaints as fraud alerts, listen to them
- There always people who can get away with a scam (for a while)

Some lessons (2)

- Security policy will always have exceptions to cope with real life
  - These workarounds create vulnerabilities
- If you have high error rate, it is hard to find fraudulent transactions
- Verify that your records correspond to external reality

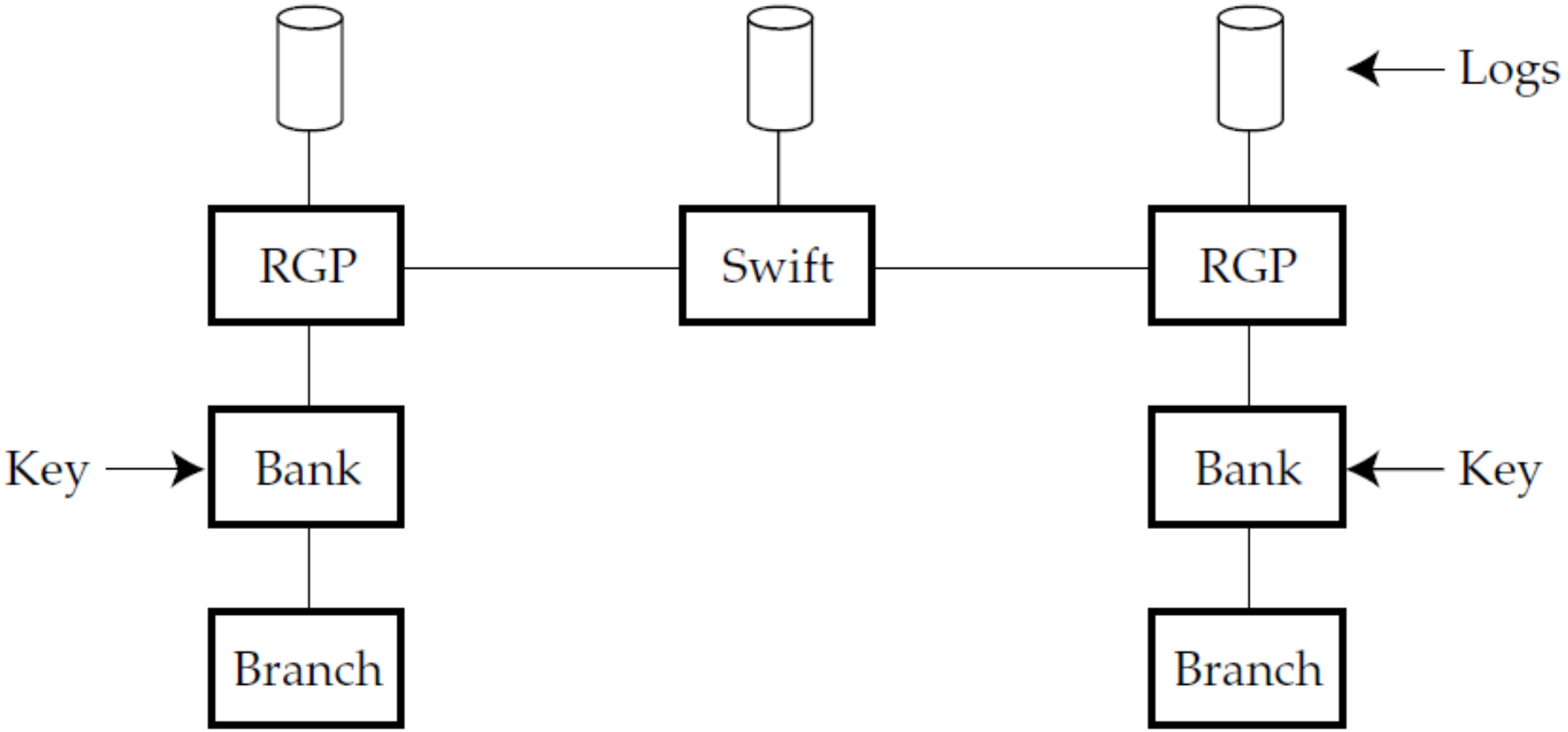
SWIFT

- Inter-bank money transfer system
  - Developed in 70s
- Banks did not want to trust SWIFT
- Integrity mechanisms separate from confidentiality
  - In some countries encryption was illegal
- Digital signatures were not invented
  - Non-repudiation was done without them
- Clark-Wilson type controls

Message protection

- MAC was used for message authentication
  - Parties need to share a secret key
  - Authenticity of a message cannot be proven to third party
- Keys were managed end-to-end
  - Manages physically carried the keys

SWIFT architecture



SWIFT architecture (2)

- Swift provided non-repudiation service
- RGP (regional general processor) and SWIFT centre logged the message
- Confidentiality was done between banks and RGP and between RGPs and central node
  - All the SWIFT nodes could see message contents

SWIFT architecture (3)

- Messages can be entered via special terminals
- For big banks, message sending was integrated with the main system
- Shared control when sending message
  - One person enters, second person checks, third person authorizes
- Transactions checked against daily statements

SWIFT experiences

- The cryptography is quite low-tech
  - However, this does not usually matter
  - Physical control, logging, contracts, audits, limits, procedures, approvals, money laundering controls
- Naive programmers insert messages into the queue
  - ... and are caught by other security measures

SWIFT experiences

- Successful attacks exploit weaknesses in procedures
- Example: letter of guarantee
  - Can be exchanged over SWIFT
  - Does not take part in balancing
  - Abuses are discovered much later
- Example: Stanley Rifkin stole authorization code and dictated wire transfer over the phone
  - Caught when trying to sell the diamonds

Automatic teller machines

- PIN calculation basics

Account number PAN:	`8807012345691715`
PIN key KP:	`FEFEFEFEFEFEFEFE`
Result of DES $\{PAN\}_{KP}$:	`A2CE126C69AEC82D`
$\{N\}_{KP}$ decimalized:	`0224126269042823`
Natural PIN:	`0224`
Offset:	`6565`
Customer PIN:	`6789`

ATM basics

- All the operations on PIN are performed in tamper-resistant hardware modules
  - PIN and card can be produced separately
- Each ATM contains hardware module that stores terminal master key
  - Usually key is split into two components and entered by two different persons

ATM basics (2)

- For offline PIN verification, the PIN key is sent to ATM, encrypted with terminal master key
- For online PIN verification, the PIN is sent to central security module, encrypted with the terminal master key

Inter-bank verification

- Banks can exchange communication keys bilaterally
- Organizations like VISA exchange keys with each bank separately
- For inter-bank verification:
  - PIN is sent to central computer with terminal master key
  - central computer sends to VISA with VISA's key
  - VISA re-encrypts it with key of other bank

Summary

- Clark-Wilson security policy is mainly concerned with maintaining invariant on the system's state
- Dual control can be implemented serially or in parallel
- With inter-organization transactions, non-repudiation is required
- Embed security measures into normal working procedures

Home reading!

- Read chapter 10 of Ross Anderson's „Security Engineering”
  - Especially second half about ATM and credit cards

http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c